

Presented to the Court by the foreman of the
Grand Jury in open Court, in the presence
of the Grand Jury and FILED in the U.S.
DISTRICT COURT at Seattle, Washington

August 20, 2020

WILLIAM M. McCOOL, Clerk

By Shawn Katter Deputy

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,
Plaintiff,

NO. CR20-127 RSL

INDICTMENT

v.

(1) MAX LOUARN,
aka "MAXiMiLiEN"
aka "Julien Ambroise,"

(2) YUANNING CHEN,
aka "Yuan Ning Chen"
aka "Velison Chen"
aka "100+1"
aka "Jingui Chen,"

(3) GARY BOWSER,
aka "GaryOPA,"

Defendants.

The Grand Jury charges that:

DEFINITIONS

1. **Videogame:** A videogame is a software game designed to be played through a computer system. Videogames can be sold as physical titles, such as game cartridges or discs, or as digital titles. Most commercial videogame titles integrate

INDICTMENT - 1

United States v. Louarn, et al.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1 | valuable intellectual property and are protected by U.S. copyright and trademark law.
2 | The sale and use of such videogame titles are governed by contractual arrangements and
3 | licensing agreements, and generate revenue for videogame developers, publishers,
4 | retailers and console manufacturers, among others.

5 | 2. **Technological Measure:** A “technological measure” refers to a measure
6 | designed to control access to or use of a protected work. “[A] technological measure
7 | ‘effectively controls access to a [copyrighted] work’ if the measure, in the ordinary
8 | course of its operation, requires the application of information, or a process or a
9 | treatment, with the authority of the copyright owner, to gain access to the work.”
10 | 17 U.S.C. § 1201(a)(3)(B).

11 | 3. **Circumvention:** “Circumvention” is the act of bypassing, avoiding,
12 | removing, deactivating, or impairing a technological measure or device that controls
13 | access to a work protected by U.S. copyright law.

14 | 4. **Circumvention device:** A “circumvention device” is an apparatus or
15 | software designed to bypass, avoid, remove, deactivate, or impair a technological
16 | measure that controls access to or use of a protected work without the authority of the
17 | copyright owner.

18 | 5. **Internet Protocol (“IP”) Address:** An IP address is a unique numeric
19 | address used by devices, such as computers, on the Internet. Every device connected to
20 | the Internet must be assigned an IP address so that Internet traffic sent from and directed
21 | to that device may be directed properly from its source to its destination. Most Internet
22 | service providers control a range of IP addresses.

23 | 6. **Server:** A “server” is a computer that provides services for other
24 | computers connected to it via a network or the Internet. The computers that use the
25 | server’s services are sometimes called “clients.” Servers can be physically located
26 | anywhere with a network connection that may be reached by the clients; for example, it is
27 | not uncommon for a server to be located hundreds (or even thousands) of miles away
28 | from the client computers.

1 7. **Firmware:** “Firmware” generally refers to a software program embedded
2 in a hardware device that provides instructions regarding how the hardware functions and
3 communicates with other devices and software. Firmware is usually stored in the read-
4 only memory of the device and cannot be erased or rewritten.

5 8. **Encryption:** “Encryption” is the use of a cryptographic method to protect
6 sensitive data. Typically, sensitive data is encrypted using an algorithm to make it
7 readable only by authorized users who possess the key or cipher needed to decrypt the
8 data.

9 9. **Scrambling:** “Scrambling” is a data obfuscation technique that involves
10 the rearranging of data in a predetermined way such that it can be restored by an
11 authorized user.

12 10. **Exploit:** An “exploit” is code that takes advantage of a vulnerability or
13 security flaw to cause unintended or unanticipated behavior to occur on computer
14 software, firmware, or hardware.

15 11. **ROM:** “ROM” typically stands for “read-only memory.” However, ROM
16 is generally understood in the videogaming community to refer to an unauthorized or
17 pirated copy of a videogame title that can take the form of read-only memory files or
18 read-only memory images. Depending on its nature, a ROM can be played on consoles,
19 computers, phones and other devices often through the use of a circumvention device or
20 an “emulator.”

21 12. **Emulator:** An “emulator” is a hardware device or software program that
22 enables a computer system to mimic the functions of another computer system.

23 13. **Mod Chip:** A “mod chip” or “modchip,” in the context of the videogaming
24 community, is a physical device used to circumvent technological measures on
25 videogame consoles.

26 14. **Home Brew:** “Home brew” or “homebrew,” in the context of the
27 videogaming community, is a term coined by gaming enthusiasts who seek to add
28 functions to videogame consoles beyond the parameters set by the hardware

1 manufacturer. Homebrew can involve expanding the functions of a console to allow the
2 device to do more than just play games. Homebrew enthusiasts also develop games that
3 can be played on the modified consoles. Certain homebrew games are entirely original
4 games, while others modify copyrighted works or use trademarked characters without the
5 rights holders' consent.

6 15. **Pirated:** "Piracy" refers to the unauthorized and illegal reproduction or
7 distribution of works protected by copyright or trademark law. "Pirated" software is
8 protected software that has been copied, modified, used, or sold without permission.
9 Software piracy denies copyright holders of due compensation for use of their creative
10 works.

11 INTRODUCTORY ALLEGATIONS

12 16. The defendants, MAX LOUARN, aka "MAXiMiLiEN," aka "Julien
13 Ambroise," YUANNING CHEN, aka "Yuan Ning Chen," aka "Velison Chen," aka
14 "100+1," aka "Jingui Chen," and GARY BOWSER, aka "GaryOPA," and others known
15 and unknown to the Grand Jury, were part of a financially-motivated hacking group that
16 ran a criminal enterprise that developed, manufactured, marketed, and sold a wide variety
17 of circumvention devices.

18 17. The enterprise used various names and brands, including, among others,
19 "Team Xecuter," "Axiogame.com," "Maxconsole.com," and "China Distribution," to
20 facilitate the sale of the circumvention devices. The enterprise designed these devices
21 primarily to circumvent technological measures in a manner that allowed users to play
22 pirated versions of copyrighted videogames, also known as "ROMs." The devices
23 mimicked legitimate gameplay on consoles and, in certain instances, surreptitiously
24 accessed at least one videogame company's servers and online gaming without
25 authorization. To facilitate the sales of their circumvention devices, the enterprise
26 supported and promoted online ROM repositories.
27
28

1 **A. Background on the Videogame Industry**

2 18. The defendants carried out a scheme that sought to profit from, among
3 other things, the illegal use of pirated videogames on popular videogame consoles.
4 Videogame consoles are home entertainment computers designed primarily to play
5 copyright-protected videogames in proprietary formats. Consoles typically come in the
6 form of either home consoles designed for residential gameplay, or handheld consoles
7 designed for mobile gameplay. Traditionally, videogame consoles were designed to play
8 game cartridges, cards, or discs. However, videogame manufacturers have invested
9 substantial resources in developing online marketplaces in which customers can use their
10 consoles to access an online account to, among other things, purchase digital game titles
11 and services. Moreover, gaming companies have developed extensive online ecosystems,
12 hosted on servers maintained by or leased by gaming companies, in which customers can
13 use their game consoles to receive updates, unlock game features, exchange messages,
14 and play games online with other players.

15 19. The design, development, and promotion of videogame consoles (and the
16 associated online features) requires a tremendous investment of time and financial
17 resources. Console manufacturers like Nintendo, Sony, and Microsoft, often manufacture
18 game consoles with small profit margins. To recoup these costs, manufacturers depend
19 on the stream of revenue that flows after a customer purchases a console. The customer's
20 purchase of licenses to play copyright-protected videogames accounts for the majority of
21 that revenue stream.

22 20. Beyond the costs to develop videogame consoles, individual videogame
23 titles themselves can take years to develop at the cost of millions of dollars. Many game
24 titles are designed to be played exclusively on a specific manufacturer's console. For
25 example, Nintendo has a family of game titles that cannot be played on the Sony
26 PlayStation or the Microsoft Xbox.

27 21. According to the Entertainment Software Association's ("ESA") 2019
28 report on "Essential Facts About the Computer and Video Game Industry," 65% of

1 American adults play videogames, and 49% of those adults use a dedicated game
2 console. ESA's report indicates that Americans spent far more on videogame content
3 than physical hardware devices in 2018. Whereas Americans spent \$5.1 billion on
4 gaming hardware, they spent \$35.8 billion on videogame content.

5 22. Commercial videogame titles represent a bundle of contractual rights and
6 licenses. According to these rights and licenses, revenue from the distribution and sale of
7 commercial videogame titles flows to console manufacturers, developers who finance
8 and create the titles, publishers who release and market the titles, holders of copyrighted
9 and trademarked material integrated in the titles, and retailers who sell the titles to
10 customers either online or through brick and mortar stores. These studios, companies,
11 and other entities will be referred to as the "victim companies" throughout this
12 Indictment.

13 23. The use of major consoles to play copyrighted videogame titles is typically
14 governed by end user license agreements. These agreements allow a user to purchase a
15 limited license to use protected software on the consoles, such as the console's operating
16 system and individual videogame titles. These agreements also prohibit the user from,
17 among other things, duplicating, reproducing, modifying, and selling the software.

18 24. To further protect their intellectual property against videogame piracy, and
19 to ensure that only authorized and licensed videogames can be played on legitimate
20 devices, console manufacturers and game developers implement technological measures
21 to prevent the use of unauthorized firmware and the playing of pirated videogames.
22 These technological measures range from how game cartridges are designed, to
23 cryptographic keys that are placed on the software. Due to the effectiveness of
24 technological measures on modern videogame consoles made by leading companies,
25 pirated ROMs typically cannot be played on these consoles without the use of a
26 circumvention device, such as the devices developed and distributed by the enterprise.

27 25. Console manufacturers also have developed techniques, such as the use of
28 authentication processes, to detect if a console is playing a counterfeit game when that

1 console connects to a console manufacturer's servers. This allows console manufacturers
2 to flag or ban consoles that are engaged in such activity.

3 26. Console manufacturers and game developers rely on the protections
4 provided by trademark and copyright law. Copyright and trademark notices typically are
5 displayed when games and firmware software are booted up. Copyright and trademark
6 notices are also displayed prominently on the packaging for consoles and videogames.

7 27. The theft of intellectual property causes substantial damage to victim
8 companies. Circumvention devices are predominantly designed to allow users to play
9 pirated videogame titles. Consequently, the manufacturers and sellers of circumvention
10 devices aim to profit from the sale of devices that are designed to deprive victim
11 companies of the stream of revenue they are entitled to receive from the use of the
12 videogame titles.

13 28. In addition, pirated videogame titles sometimes permit the users of those
14 pirated videogame titles to manipulate games, which can affect the gameplay of
15 legitimate users in an online, multiplayer environment. Thus, the circulation and use of
16 pirated videogame titles tarnishes brand names and erodes the goodwill that victim
17 companies have developed with their legitimate customers.

18 **B. The Defendants' Roles**

19 29. The enterprise was led by a core group of individuals who have worked to
20 profit from software piracy for numerous years under a variety of team names. As
21 experienced operators in the illegal modchip industry, the leaders of the enterprise knew
22 that U.S. law prohibited both the distribution of ROMs, and the distribution and use of
23 devices that circumvented technological measures on game consoles.

24 30. Defendant MAX LOUARN, aka "MAXiMiLiEN," aka "Julien Ambroise,"
25 was a leader of the enterprise who recruited investors and exploit developers, made
26 strategic business decisions, finalized product design, and financed projects. LOUARN
27 played a critical role in establishing wholesale distribution chains and linking the
28 enterprise's manufacturer with various resellers around the world. LOUARN also

1 | oversaw the development and administration of at least one of those resellers, an online
2 | modchip marketplace called Axiogame.com.

3 | 31. Defendant YUANNING CHEN, aka "Yuan Ning Chen," aka "Velison
4 | Chen," aka "100+1," aka "Jingui Chen," provided financing and strategic guidance for
5 | the development of the enterprise's circumvention devices. CHEN oversaw the
6 | management of a manufacturing and distribution company called "China Distribution,"
7 | aka "ChinaDistrib," that held itself out as the official wholesale distributor of many of the
8 | circumvention devices. In addition, the enterprise held CHEN out as the public operator
9 | of Axiogame.com.

10 | 32. Defendant GARY BOWSER, aka "GaryOPA," was responsible for
11 | developing circumvention devices and marketing those devices. BOWSER was the
12 | administrator of multiple websites operated by the enterprise, including a website called
13 | maxconsole.com, which served as a central location for the enterprise to introduce
14 | reviews, advertisements, and support forums for circumvention devices and the resellers
15 | who were selling the devices in various countries.

16 | **C. The Development and Distribution of Circumvention Devices**

17 | 33. The conspiracy developed and sold numerous circumvention devices for
18 | leading videogame consoles. The sale of these circumvention devices involved the
19 | interstate and international transmission of electronic communications about the devices,
20 | in addition to the interstate and international shipment of the actual devices, to locations
21 | in the Western District of Washington and elsewhere.

22 | 34. Although it would have been more efficient for the enterprise to use a
23 | single brand to develop, market, and distribute its products, the enterprise chose to use a
24 | wide variety of brands, websites, and distribution channels. The enterprise used this
25 | fragmented approach to protect the overall enterprise in the event that one device or
26 | brand were to be targeted by gaming companies, financial institutions, and law
27 | enforcement.
28 |

1 35. The enterprise recruited and hired developers to create and design
2 circumvention devices. From time to time, the enterprise sought to partner with
3 individual hackers or groups of hackers who had already developed an exploit for a
4 particular game console. Subsequently, LOUARN and CHEN would arrange for the
5 manufacture and distribution of the devices that targeted the exploit.

6 36. To protect its projects from other teams of hackers and law enforcement,
7 the enterprise regularly used encrypted means of communication. Among other channels
8 of communication, the enterprise utilized applications offering end-to-end encryption,
9 such as Signal and Telegram, and employed PGP encryption in sensitive email
10 communications.

11 37. The enterprise deployed a variety of techniques to mask and protect servers
12 under the enterprise's control. Among other things, the enterprise utilized technology
13 that allowed members to remain anonymous or immune from legal enforcement actions,
14 such as reverse proxies and bulletproof hosting providers.

15 38. The commercial success of the enterprise's circumvention devices
16 depended primarily on the availability of pirated ROMs. Otherwise, users would have
17 been forced to copy their own ROMs from game titles. Accordingly, the enterprise
18 undertook efforts to create and support online ROM libraries that could be used by the
19 enterprise's customers. The enterprise directed users to ROM libraries through the
20 enterprise's website, maxconsole.com. Additionally, some of the enterprise's resellers
21 sold circumvention devices as a package with ROMs of game titles or otherwise offered
22 ROMs directly or indirectly to customers.

23 39. At times, the enterprise also attempted to cloak its illegal activity with a
24 purported desire to support homebrew enthusiasts who wanted to design their own
25 games. However, the predominant design of the enterprise's products was to allow
26 purchasers to play pirated ROMs.

D. The Team Xecuter Brand

40. Beginning at a time unknown, but no later than June 2015, the defendants and their co-conspirators operated a significant portion of their illegal enterprise under the Team Xecuter brand. Team Xecuter held itself out as a legitimate company that had broken from a dubious past. The group had a prominent presence online and operated a public website entitled, "Team Xecuter – Rocking The Video Gaming Console Scene Since 2002." The group aggressively advertised its products on various online forums and in YouTube videos.

41. The "About Us" section of the public website contained the following statement, indicating that Team Xecuter has been involved in the development of circumvention devices since 2001:

Team Xecuter have developed hardware and software for the Xbox Scene since 2001. The initial roots of the group were based on the Xbox homebrew hacking scene, however where we started as a small group of hardcore enthusiasts dealing with extremely gray area market products, we have now grown into a large electrical manufacturer that develops products for many companies around the world.

Our heart still lies within the games console community and we are always active in developing new and innovative products that we ourselves use in our gaming lives. Whereas we have long digressed from trading in areas that have now been made illegal in most countries over the years, our ambition is to continue to produce quality items at an affordable price.

42. Most of Team Xecuter's products (excluding accessories) were designed to be circumvention devices that had the purpose of allowing users to play pirated ROMs.

43. Beginning in May 2018, the enterprise began releasing a family of Team Xecuter-branded hardware devices for use on the Nintendo Switch videogame console. These devices were designed to run a custom operating system called the "SX OS." Together, the hardware device and operating system circumvented the technological measures on the Nintendo Switch and permitted users to, among other things, access and manipulate the copyrighted Nintendo Switch operating system and play pirated ROMs.

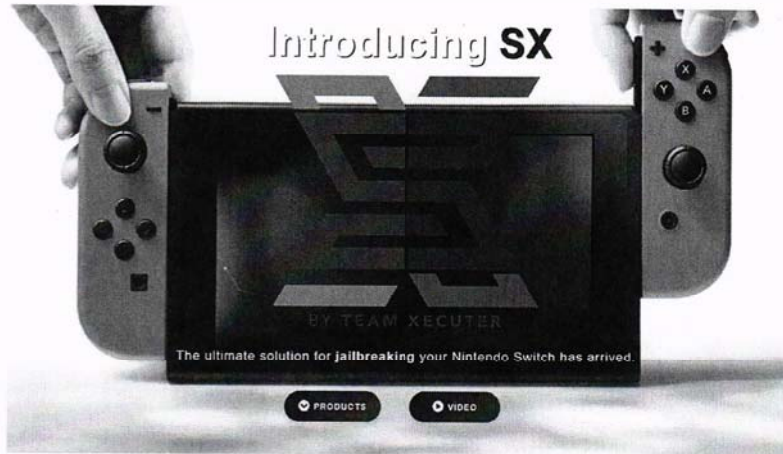
1 44. Like other Nintendo consoles, Nintendo employs a number of technological
2 measures in its Nintendo Switch consoles, game cartridges, and digitally downloaded
3 games, to protect and control access to its copyrighted works.

4 45. For example, each Nintendo Switch contains an encrypted identifier, or
5 “signature,” that is checked when the console is powered on. The firmware or operating
6 system also contains technological measures designed to ensure the operating system is
7 authorized. The Nintendo Switch will only power on normally if these technological
8 measures are confirmed as authentic.

9 46. In addition to the console-based technological measures, when a Nintendo
10 Switch attempts to connect with Nintendo’s servers, such as when a user attempts to play
11 online, purchase games, or download updates, Nintendo’s servers normally will verify the
12 console’s certificate. Typically, users are able to access Nintendo’s online services only
13 if this check is successful. Nintendo has banned specific user accounts or consoles from
14 Nintendo’s network when the authentication measures detected unauthorized use.

15 47. The Nintendo Switch also contains technological measures that protect
16 each videogame played on the Nintendo Switch. These game-based technological
17 measures use encryption and signature checks to ensure that the game is authentic and
18 that the console is authorized to operate the game.

19 48. The initial Team Xecuter-branded circumvention device for the Nintendo
20 Switch was called the “SX Pro.” The enterprise created a dedicated website,
21 sx.xecuter.com, to promote and sell the device, which it described as “[t]he ultimate
22 solution for jailbreaking your Nintendo Switch”:
23
24
25
26
27
28



49. A Nintendo Switch hacked with the SX Pro and SX OS could play virtually any pirated ROM. Many, if not all, of Team Xecuter's customers who purchased the SX Pro located pirated ROMs online, transferred unauthorized copies of those ROMs to a memory card, and used the SX Pro and the SX OS to play those ROMs.

50. The SX Pro kit consisted of the "Xecuter Jig" and the "Xecuter Dongle." The Xecuter Jig was designed to slide into the rail on the right side of the Switch console so that metal prongs on the jig covered the console pins in the rail. Powering on the Switch with the jig covering the console pins circumvented the console-based technological measures by causing the Switch to short-circuit and go into recovery mode. This interfered with the normal operation of the Nintendo Switch to interrupt and bypass the Nintendo Switch's sequence of security checks. The Xecuter Dongle was then used to upload the SX OS onto the Switch console. Subsequently, the SX OS could bypass authentication processes designed to protect both Nintendo's copyrighted material and the integrity of the company's online ecosystem.

51. To enable the SX OS to play pirated ROMs, a user generally would need to connect the Switch console to the internet to purchase a "license" from Team Xecuter to unlock the full features of the circumvention device. The SX OS license allowed users to forego purchasing a game cartridge from a retailer or a digital game from Nintendo's eShop because the full-featured SX OS bypassed the normal operation of technological measures that were designed to limit the use of the console to legitimately purchased

1 games. Among other technological measures, the SX OS circumvented an authentication
2 process that used cryptographic keys to ensure that only authorized games were played
3 on a particular Switch console.

4 52. The irony of a hacking group such as Team Xecuter using a licensing
5 scheme to protect its circumvention software from being pirated was not lost on the
6 gaming community. On June 28, 2018, the website “Ars Technica” published an article
7 titled, “Pirates Battling Pirates – Switch pirates don’t want you to pirate their piracy-
8 enabling firmware.” The article indicated that a representative of Team Xecuter
9 defended the use of the licensing scheme as a “harmless cat-and-mouse game between
10 aspiring hackers and competing teams.” Apparently, the Team Xecuter representative
11 further explained that, “[w]e do implement inconveniences to safeguard anti-tampering of
12 our SX OS boot file to remain at a competitive advantage.”

13 53. The enterprise designed the SX OS to insert itself into the legitimate
14 firmware of the Switch console. In doing so, the SX OS surreptitiously co-opted
15 functions and processes that Nintendo implemented to support legitimate gameplay on
16 the Switch consoles. Notably, the SX OS used, without authorization, and in violation of
17 the Switch console’s end user agreement, servers that Nintendo maintained to facilitate
18 internet connectivity and to authenticate the use of genuine Nintendo software. The SX
19 OS was designed to falsely represent to Nintendo’s servers that the Nintendo Switch on
20 which it was operating was using a legitimate version of the Nintendo operating system
21 and legitimate Switch videogames. In this manner, the enterprise designed the SX OS to
22 generate criminal proceeds from the fraudulent use of Switch consoles and the Nintendo
23 servers that were dedicated to support legitimate gameplay on those consoles.

24 54. On July 31, 2018, investigators in the Western District of Washington
25 purchased an SX Pro Mod Kit from www.switchsx.com, which the enterprise identified
26 on team-xecuter.com as an ‘authorized’ reseller. The modchip subsequently was shipped
27 from Rockville, Maryland to Mukilteo, Washington.
28

1 55. On or about March 13, 2020, investigators in Seattle, Washington installed
2 the SX OS, purchased from different 'authorized' resellers, onto separate Switch
3 consoles. During the installation process, the SX OS prompted the investigators to
4 activate the licenses for the SX OS on each console. The activation process subsequently
5 caused the Switch consoles to connect to servers located in Portland, Oregon that
6 Nintendo maintained to facilitate the internet connectivity of consoles being used for
7 legitimate purposes. Subsequently, the consoles connected to reverse proxy servers
8 outside of Washington State that the enterprise used to shield the location of its actual
9 servers.

10 56. During the installation of the SX OS and the activation of the licenses on
11 the consoles, the SX OS circumvented technological measures that were designed to
12 protect Nintendo's intellectual property. Among other things, the consoles connected
13 with, and evaded detection by, servers that Nintendo maintained to authenticate
14 legitimate use of Nintendo hardware and software, and thereby control access to
15 copyrighted material. This authentication process served multiple purposes, including,
16 but not limited to, fighting piracy and maintaining the integrity of Nintendo's software
17 and its online ecosystem. In summary, the SX OS improperly accessed Nintendo's
18 servers to activate the SX OS licenses on each console, and otherwise caused multiple
19 interstate wires.

20 57. Nintendo undertook various efforts in response to the enterprise's release of
21 the SX Pro and SX OS. In response, Team Xecuter released new devices or updated the
22 enterprise's software to permit further circumvention.

23 58. For example, in or around June 2018, Nintendo released a new version of
24 the Nintendo Switch with updated technological measures to prevent the console from
25 being hacked by the SX Pro and SX OS. Furthermore, in or around September 2019,
26 Nintendo released a new console, the Nintendo Switch Lite, that was produced with the
27 updated technological measures to, among other things, address circumvention devices
28 such as the SX Pro and SX OS. On or about December 28, 2019, the enterprise

1 | responded by announcing the development of new circumvention devices, posting a
2 | video to their blog, Team-Xecuter.com showing the SX OS purportedly running on the
3 | Nintendo Switch Lite. The enterprise boasted, “We rocked the Switch in 2019 and with
4 | the year soon over, here is a little teaser of one of the things to come early 2020! Enjoy!”

5 | 59. In or around April 2020, the enterprise announced they would begin
6 | accepting pre-orders for new circumvention devices, called “SX Core” and “SX Lite.”
7 | The enterprise designed the SX Core to circumvent the technological measures in pre-
8 | and post-June 2018 Nintendo Switch consoles. The enterprise designed the SX Lite to
9 | circumvent the technological protection measures in the Nintendo Switch Lite. Unlike
10 | the SX Pro, these circumvention devices need to be installed inside the casing of the
11 | console.

12 | 60. The enterprise, through the axiogame.com website, explained that the SX
13 | Core works on all consoles “that currently can’t work with external usb dongles.” The
14 | enterprise also explained, through sxflashcard.com, that the “SX CORE is for hacking
15 | Nintendo Switch patched and new Nintendo Switch 2019” and that the SX Lite is “ultra
16 | simple and almost plug and play,” and that one must only “dismantle the console.”

17 | 61. In or around May 2020, the enterprise announced, through the Team
18 | Xecuter blog, that the enterprise had shipped samples of the SX Core and SX Lite to
19 | reviewers.

20 | **E. The China Distribution Brand**

21 | 62. China Distribution, aka, “China Distrib,” was the entity that the enterprise
22 | used to distribute the enterprise’s circumvention devices. The enterprise set up
23 | www.chinadistrib.com as the dedicated website for China Distribution. The website
24 | provided information primarily to resellers who wished to make wholesale purchases of
25 | the enterprise’s modchips. LOUARN played a central role in managing wholesale
26 | relationships and responding to customer complaints.

27 | 63. The enterprise periodically circulated digital newsletters describing new
28 | products and updates to existing products. For example, on or about April 3, 2018, the

1 enterprise circulated a newsletter indicating that China Distribution would be taking
2 preorders for Team Xecuter's circumvention device for the Nintendo Switch. The
3 newsletter warned: "Beware of clones/cheap copies. China Distrib is the only distributor
4 that guarantees that all its products come directly from the manufacturer." The newsletter
5 also indicated China Distribution was the "[o]fficial distributor for" the following
6 products:

7 N2/Amiiqo
8 Stargate-3ds
9 Team Xecuter
10 Cobra
11 Gateway
12 Kocasata
13 E3
14 Maximus
15 Progskeet
16 Swap Magic
17 Wode
18 and many more ...

16 64. Despite the enterprise's efforts to create the appearance of legitimacy, the
17 leaders of the enterprise were aware of the illegality of the circumvention devices they
18 developed and distributed. Among other efforts to frustrate enforcement efforts, the
19 enterprise concealed the nature of the circumvention devices that it shipped to various
20 countries, including to the United States. On customs declaration forms for shipments,
21 the enterprise would regularly use false merchandise descriptions, tariff classifications,
22 and value descriptions to evade detection. For example, on or about June 15, 2018,
23 LOUARN sent an email to CHEN regarding the shipment of 1,000 units of the SX Pro
24 circumvention device to a reseller based in Cyprus. LOUARN indicated that CHEN
25 should declare a subsequent shipment of the device as a "memory card adaptor" at a
26 "value of \$0.20 each."
27
28

F. Axiogame.com and Other Resellers

65. The enterprise also sold its circumvention devices directly to individual consumers through its own online platforms.

66. For example, LOUARN and CHEN sold modchips through an online marketplace called axiogame.com. This website sold modchips developed by the enterprise in addition to a variety of gaming accessories. The “About us” section of the website explained:

Axiogame.com is your dedicated electronic shop since 2001, delivering to world with free shipping all your favorite videogame and electronic products.

We offer fast shipment, strong customer support available 6 days a week by mail and the best prices in the industry.

Payments are secure and all major credit/debit cards are accepted.

If you have any question, please feel free to contact us, we will make sure to answer you with as much details as possible and we look forward to add you as another satisfied customer.

Axiogame.com is operated by:

Mr. Chen

67. In addition to operating the website of at least one reseller, LOUARN expanded the reach of the enterprise by establishing wholesale distribution chains to other resellers. The enterprise identified and promoted its authorized resellers on websites controlled by the enterprise, such as maxconsole.com and team-xecuter.com, in addition to dedicated marketing pages that the enterprise created for its main products.

G. Examples of Other Devices Trafficked by the Enterprise

68. The enterprise utilized different brands and product names to silo its products and to thereby insulate the overall enterprise from anti-piracy efforts.

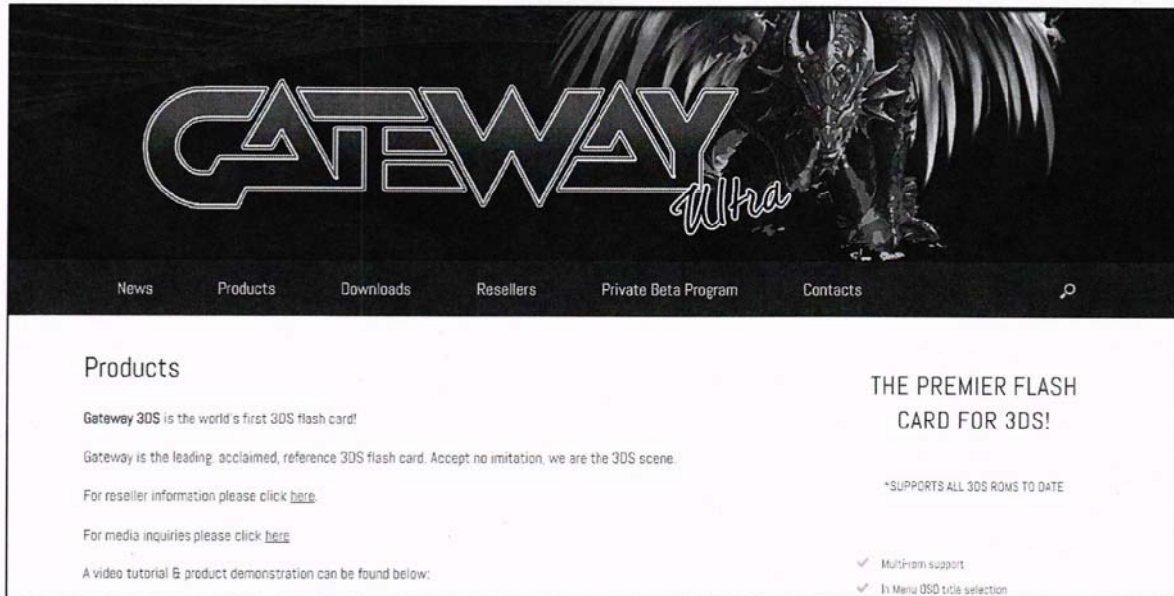
1 **1. Gateway 3DS**

2 69. On or about June 2013, the enterprise began marketing and distributing a
3 circumvention device called the “Gateway 3DS” that was designed to allow purchasers to
4 play pirated ROMs on the Nintendo 3DS.

5 70. Nintendo employs a number of technological measures in its Nintendo 3DS
6 consoles and Nintendo 3DS game cards to protect and control access to its copyrighted
7 videogames. Specifically, the technological measures used by Nintendo to control
8 protected works include: (1) the unique design of Nintendo 3DS game cards, to include
9 their size, shape, and electrical connection which are unlike those of standard
10 commercially available memory cards; (2) boot up security checks performed by
11 software in the console’s internal memory and on the game cards; and (3) encryption and
12 scrambling of commands and data exchanged between the console and game cards.
13 Unless these technological measures are satisfied, the Nintendo 3DS will not run any
14 software from the inserted game card.

15 71. The Gateway 3DS circumvented these technological measures in multiple
16 ways. The Gateway 3DS was designed to resemble the normal game card for the
17 Nintendo 3DS, with its unique size, shape, and electrical connection. However, unlike a
18 legitimate cartridge, the Gateway 3DS contained a slot in which a Micro SD card could
19 be inserted. This allowed the user to upload numerous ROMs onto a Micro SD card so
20 that they could be played on the Nintendo 3DS through the Gateway 3DS circumvention
21 device. Furthermore, the Gateway 3DS contained software that circumvented the
22 security checks and encryption imposed by Nintendo’s technological measures, allowing
23 the user to play pirated videogame titles.

24 72. The enterprise advertised the device on a dedicated website as “THE
25 PREMIER FLASH CARD FOR THE 3DS! . . . *SUPPORTS ALL 3DS ROMS TO
26 DATE.” The “Products” page of the website contained the following advertisement:
27
28



The website contained links to user manuals in English and five other languages that provided detailed instructions on, *inter alia*, how to install the Gateway's firmware on the Nintendo 3DS and how to play pirated ROMs. Notably, the manual indicated that customers with problems should post any questions in a Gateway support forum hosted by the enterprise's website, maxconsole.com.

73. On or about April 30, 2019, investigators in the Western District of Washington purchased a Gateway circumvention device for \$48.90 from an "authorized" reseller listed on the product's dedicated webpage, gateway3ds.info. The device was subsequently shipped from China with a product description of "video game accessory" and with a declared value of \$28.00.

2. Stargate

74. In approximately August 2017, the enterprise improved upon the Gateway 3DS and launched a new device to play pirated ROMs on the Nintendo 3DS called the "Stargate." The Stargate was designed to address some of the flaws of the Gateway 3DS.

75. The Stargate circumvented the Nintendo 3DS's technological measures in many of the same ways as the Gateway 3DS. For example, like the Gateway 3DS, the Stargate resembled a legitimate game card except that it contained a slot in which a Micro SD card could be inserted to allow the user to play pirated ROMs from the Micro

SD card. The Stargate also contained software that circumvented the security checks and encryption put in place by the Nintendo 3DS's technological measures.

76. Consistent with its promotion of the Gateway device, the enterprise maintained a dedicated website to market and support the Stargate. The website advertised the Stargate as follows:



77. On or about May 7, 2019, investigators in the Western District of Washington purchased a Stargate circumvention device from an "authorized" reseller listed on the product's website, stargate-3ds.com. Prior to submitting payment and receiving the shipment, investigators exchanged multiple emails with the seller of the device regarding the purchase. For example, on or about May 6, 2019, the seller of the device sent an email identifying a payment account that was to be used to finalize the purchase. The seller also requested that the purchaser conceal the nature of the transaction from the payment processor: "here is our . . . account, send money there and leave [a] message on the order id (or order reference, please don't write anything about flashcard or our brand because of piracy), then send me the screenshot, thanks much."

3. TrueBlue Mini

78. The enterprise offered a device named the TrueBlue Mini that contained hundreds of pirated ROMs that could be played on Sony's PlayStation Classic console.

1 79. Sony released the PlayStation Classic console in 2018. This console was
2 designed to invoke the appearance of the vintage versions of the PlayStation. However,
3 unlike the vintage versions, the PlayStation Classic came pre-installed with legitimate
4 versions of the vintage videogames.

5 80. The TrueBlue Mini was a USB drive that could be plugged into the
6 PlayStation classic to allow the user to play ROMs stored on the TrueBlue Mini. It
7 thereby circumvented the technological measures that limited the PlayStation Classic to
8 the pre-installed videogames.

9 81. On or about October 29, 2019, China Distribution circulated a newsletter
10 announcing that the enterprise would be selling five different versions of the TrueBlue
11 Mini that would come with different selections of pirated ROMs:

12 True Blue mini (for PSX Classic) is now available in 5 packs! Yes, they
13 just added a new mega pack (200 games) called 'Overdose' which is
14 shipping as we speak. For those who don't know, True Blue mini is a
15 custom thumb drive (memory stick) that is plug and play and adds hundreds
16 of games to your PSX classic. Nothing to do, just plug & play and enjoy all
17 the Playstation classics on your mini console. . . We cn [sic] believe with
18 this new mega pack we might break record sales (and in fact this is the
19 highest production batch they made[.].)

20 82. The same newsletter announced that China Distribution was preparing to
21 distribute a version of the TrueBlue Mini for the SEGA Mega Drive Mini console that
22 would include 1,000 pirated ROMs of Sega Games:

23 Talking about True Blue Mini, we can't take preorders yet as we don't have
24 [the] final price (but retail should be around \$25), but a True Blue Mini for
25 Sega Mega Drive Mini is in the works, and because of smaller game size,
26 the pack will include 1000 original Sega Games!!! Basically with this
27 cheap accessory, your MegaDrive Mini will hold the full collection of all
28 Sega games. Check on China Distrib for availability, it will be w[i]thin a
few weeks.

83. As with other products developed by the enterprise, the TrueBlue Mini was
marketed through a dedicated webpage, www.truebluemin.com. The website provided

links to a worldwide network of modchip marketplaces from which the TrueBlue Mini could be purchased. The website contained the following image of the TrueBlue Mini:



84. On or about April 25, 2020, investigators in the Western District of Washington purchased a True Blue Mini Overdose Pack circumvention device from an authorized reseller listed on the product's website, truebluemini.com. Prior to receiving the shipment, investigators exchanged multiple emails regarding the purchase. The product was shipped from China, but the shipping package used to deliver the product indicated that the package was shipped by a "Jon," with an address in Auburn, Alabama.

4. Classic2Magic

85. In approximately August 2018, the enterprise released a device called the "Classic2Magic," or "C2M," that was designed to circumvent technological measures employed by Nintendo and to otherwise facilitate the playing of pirated ROMs on Nintendo's Super Nintendo Entertainment System Classic Edition.

86. Nintendo released the Super Nintendo Entertainment System Classic Edition in 2017. Although this console was designed to invoke the appearance of the vintage versions of the Super Nintendo Entertainment System ("SNES"), it was different in several respects. It was smaller than the vintage versions, such that the proprietary shape of the vintage videogame cartridges could not fit. Consequently, the new console came pre-installed with legitimate versions of the vintage videogames.

1 87. Although the Classic2Magic purported to be an adapter that allowed the
2 user to play original versions of videogame cartridges on the newly released consoles, it
3 was also marketed to support the creation and use of pirated ROMs.

4 88. First, the Classic2Magic allowed users to make unauthorized copies of the
5 original videogame cartridge and to save those versions onto a USB drive. As with other
6 videogames for other Nintendo consoles, the videogame cartridges for the original Super
7 Nintendo Entertainment System had a unique design, to include their size, shape, and
8 electrical connection, which are unlike those of standard commercially available memory
9 devices. This technological measure was designed to limit the use of the console to
10 authorized copies of videogame cartridges. The Classic2Magic was designed to
11 circumvent this technological measure by allowing users to impermissibly duplicate
12 copyrighted material.

13 89. Second, the Classic2Magic contained a USB port that allowed the user to
14 play ROMs that had been downloaded onto a USB device, thereby circumventing the
15 technological measures that limited the console to operating only the pre-installed
16 videogames. On the website axiogame.com, the enterprise advertised that using the
17 Classic2Magic was “[a]s easy as copying a file onto a usb drive” and that the device
18 supported “game ROMs from any region.”

19 90. In addition to selling the Classic2Magic on a variety of online
20 marketplaces, the enterprise advertised the circumvention device on classic2magic.com.
21 The website had the following picture of the device, connected to a Nintendo console:
22
23
24
25
26
27
28



91. The website indicated that "Game ROMs for other systems are supported via extra emulators," including the following:

Arcade Games, Atari 2600, Atari 7800, Atari Lynx, Bandai WonderSwan, Bandai WonderSwan Color, Game Boy, Game Boy Color, Game Boy Advance, Nintendo 64, Nintendo Entertainment System (NES), Super Nintendo, Nintendo Virtual Boy, Intellivision, Sega Master System, Sega Game Gear, Sega Megadrive / Genesis, Sega 32X, Neo Geo Pocket, Neo Geo Pocket Color, PCEngine TurboGrafx, PCEngine SuperGrafx Vectrex.

1 92. The enterprise supported the creation of ROM libraries that would support
2 the Classic2Magic and other circumvention devices. For example, on or about October
3 15, 2018, BOWSER sent an email explaining that the enterprise's support of the
4 translation of pirated ROMs from the Japanese market was important because "these
5 roms will help increase the market of 'c2m', plus also for [the] next upcoming retro
6 product 700in1 which is now in the [final] . . . stage of hardware [development], as a lot
7 of classic gamers wish to play japan roms in north/south America . . ." Indeed, on
8 classic2magic.com, the enterprise provided a link to a website "to access all Game ROMs
9 (full games) for all systems supported, cheat codes." The link led to the enterprise's
10 website, maxconsole.com

11 93. To help launch the Classic2Magic, the enterprise sent review models to
12 generate favorable coverage and to promote the device's legitimacy. On or about
13 September 1, 2018, BOWSER sent an email explaining that:

14 since this product is both legit and grey area, we [are] hoping this extra
15 advance push with videos of people talking and demo'ing its great range of
16 users, it will help to get more resellers onboard and news coverage on big
17 sites like engadget and ign, and papwork for selling it via Amazon also is
ongoing . . .

18 94. In approximately December 2019, the enterprise announced on
19 maxconsole.com that the Classic2Magic had a new feature that would allow users to
20 connect the Classic2Magic to the Nintendo Switch. The announcement explained:

21 Yes, you can now play your original SNES cartridges directly on your
22 Nintendo Switch with Classic 2 Magic! . . . The only requirement is that
23 your Nintendo Switch has Team Xecuter's SX OS installed (for USB-
24 support) . . . Hours of retro gaming for your Nintendo Switch and the
ultimate wow effect for your geeky friends!

25 95. On or about February 27, 2020, investigators purchased 15 Classic2Magic
26 devices from the enterprise's website, ChinaDistrib.com, that subsequently were shipped
27 from China to Bellingham, Washington. Prior to receiving the shipment, investigators in
28 the Western District of Washington exchanged emails with the account,

1 sales@chinadistrib.com, regarding the order. The commercial invoice for the shipment
2 misrepresented that the shipment contained duty-free USB adapters.

3 **COUNT 1**

4 **(Conspiracy to Commit Wire Fraud)**

5 **I. OFFENSE**

6 96. The factual allegations set forth in Paragraphs 1 through 95 of this
7 Indictment are re-alleged and incorporated as if fully set forth herein.

8 97. Beginning at a time unknown, but no later than May 2018, and continuing
9 through August 19, 2020, at Seattle, within the Western District of Washington, and
10 elsewhere, the defendants, MAX LOUARN, aka "MAXiMiLiEN," aka "Julien
11 Ambroise," YUANNING CHEN, aka "Yuan Ning Chen," aka "Velison Chen," aka
12 "100+1," aka "Jingui Chen," and GARY BOWSER, aka "GaryOPA," and others known
13 and unknown to the Grand Jury, did knowingly and intentionally, agree and conspire to
14 devise and execute and attempt to execute, a scheme and artifice to defraud, and for
15 obtaining money and property by means of materially false and fraudulent pretenses,
16 representations, and promises; and in executing and attempting to execute this scheme
17 and artifice, to knowingly cause to be transmitted in interstate and foreign commerce, by
18 means of wire communication, certain signs, signals and sounds as further described
19 below, in violation of Title 18, United States Code, Section 1343.

20 **II. OBJECTS OF THE CONSPIRACY**

21 98. From a time unknown, but no later than May 2018, and continuing through
22 August 19, 2020, the conspiracy used the Team Xecuter brand to release a series of
23 products, including the SX OS, the SX Pro, the SX Core, and the SX Lite, that were
24 designed to surreptitiously bypass security and authentication measures implemented by
25 Nintendo, and to thereby permit users to play pirated ROMs.

26 99. An object of the conspiracy was to fraudulently enrich the defendants, and
27 their co-conspirators, by depriving Nintendo and other victim companies of the stream of
28 revenue they were entitled to receive from the sale, copying, and use of the pirated
videogame titles that were played using the conspiracy's circumvention devices. By law,

1 these victims had the exclusive right to control the distribution of the copyrighted and
 2 trademarked property contained in these videogame titles, and to control access to those
 3 videogame titles.

4 100. An additional object of the conspiracy was to fraudulently enrich the
 5 defendants, and their co-conspirators, through the sale of SX OS licenses in a manner that
 6 coopted a process designed for legitimate gameplay and misused Nintendo's servers, and
 7 that surreptitiously circumvented technological measures that Nintendo implemented to
 8 combat piracy.

9 **III. MANNER AND MEANS OF THE CONSPIRACY**

10 101. The manner and means of the conspiracy are set forth in Paragraphs 33
 11 through 67 of this Indictment.

12 All in violation of Title 18, United States Code, Section 1349.

14 **COUNTS 2 - 5** 15 **(Wire Fraud)**

16 102. The factual allegations set forth in Paragraphs 1 through 101 of this
 17 Indictment are re-alleged and incorporated as if fully set forth herein.

18 **I. SCHEME AND ARTIFICE TO DEFRAUD**

19 103. Beginning at a time unknown, but no later than May 2018, and continuing
 20 through August 19, 2020, at Seattle, within the Western District of Washington, and
 21 elsewhere, the defendants, MAX LOUARN, aka "MAXiMiLiEN," aka "Julien
 22 Ambroise," YUANNING CHEN, aka "Yuan Ning Chen," aka "Velison Chen," aka
 23 "100+1," aka "Jingui Chen," and GARY BOWSER, aka "GaryOPA," and others known
 24 and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to
 25 defraud and to obtain money and property by means of materially false and fraudulent
 26 pretenses, representations and promises.

27 104. An object of the scheme was to fraudulently enrich the defendants, and
 28 their co-conspirators, by depriving Nintendo and other victim companies of the stream of
 revenue they were entitled to receive from the sale, copying, and use of the pirated

videogame titles that were played using the enterprise's circumvention devices. An additional object of the conspiracy was to fraudulently enrich the defendants, and their co-conspirators, through the sale of SX OS licenses in a manner that coopted a process designed for legitimate gameplay and misused Nintendo's servers, and that surreptitiously circumvented technological measures that Nintendo implemented to combat piracy.

II. MANNER AND MEANS OF SCHEME TO DEFRAUD

105. The manner and means of the scheme and artifice to defraud are set forth in Paragraphs 16 through 95 of this Indictment.

III. EXECUTION OF SCHEME TO DEFRAUD

106. On or about the dates set forth below, at Seattle, within the Western District of Washington, and elsewhere, the defendants, and others known and unknown to the Grand Jury, having devised a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, did knowingly transmit and cause to be transmitted writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme, by means of wire communication in interstate and foreign commerce, including the following transmissions, each of which constitutes a separate count:

| Count | Approximate Date | Wire Communication |
|-------|------------------|---|
| 2 | March 13, 2020 | Connection of a Switch console running SX OS, through an SX Pro, in Seattle, Washington, to IP address 23.194.212.115 located in Portland, Oregon. |
| 3 | March 13, 2020 | Connection of a Switch console running SX OS, through an SX Pro, in Seattle, Washington, to IP addresses 104.24.105.66 and 104.24.104.66 located outside of Washington State. |

| Count | Approximate Date | Wire Communication |
|-------|------------------|---|
| 4 | March 13, 2020 | Connection of a Switch console running SX OS, through an SX Pro, in Seattle, Washington, to IP address 23.35.98.34 located in Portland, Oregon. |
| 5 | March 13, 2020 | Connection of a Switch console running SX OS, through an SX Pro, in Seattle, Washington, to IP addresses 104.24.105.66 and 104.24.104.66 located outside of Washington State. |

All in violation of Title 18, United States Code, Section 1343.

COUNT 6
**(Conspiracy to Circumvent Technological Measures and to
Traffic in Circumvention Devices)**

107. The factual allegations set forth in Paragraphs 1 through 95 of this Indictment are re-alleged and incorporated as if fully set forth herein.

I. OFFENSE

108. Beginning at a time unknown, but no later than June 2013, and continuing through August 19, 2020, at Seattle, within the Western District of Washington, and elsewhere, the defendants, MAX LOUARN, aka "MAXiMiLiEN," aka "Julien Ambroise," YUANNING CHEN, aka "Yuan Ning Chen," aka "Velison Chen," aka "100+1," aka "Jingui Chen," and GARY BOWSER, aka "GaryOPA," and others known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate and agree together to commit offenses against the United States, to wit:

a. Knowingly and willfully, and for purpose of private financial gain, circumventing a technological measure that effectively controls access to a work protected under Title 17 of the United States Code, in violation of Title 17, United States Code, Sections 1201(a)(1)(A), and 1204(a)(1); and

b. Knowingly and willfully, and for purposes of private financial gain, manufacturing, importing, offering to the public, and trafficking in a technology, product, service, device, component, and part thereof, that is primarily designed and produced for the purpose of circumventing a technological measure that effectively controlled access to a work protected under Title 17 of the United States Code, in violation of Title 17, United States Code, Sections 1201(a)(2)(A) and 1204(a)(1).

II. OBJECTS OF THE CONSPIRACY

109. The objects of the conspiracy were to generate revenue from the distribution and sale of circumventions devices; frustrate enforcement efforts undertaken by console manufacturers; conceal the nature and scope of the criminal enterprise from law enforcement, customs officials, and financial institutions; and generate advertising revenue from websites under the conspiracy's control.

III. MANNER AND MEANS OF THE CONSPIRACY

110. The manner and means are set forth in Paragraphs 33 through 95 of the Indictment.

IV. OVERT ACTS

111. In furtherance of the conspiracy, and to achieve the objects thereof, the defendants, and others known and unknown to the Grand Jury, did commit and cause to be committed, the following overt acts, among others, at Seattle, in the Western District of Washington and elsewhere:

112. On or about June 24, 2015, LOUARN sent an email to a co-conspirator who wanted to move the location of the conspiracy's web server, which read in part:

You are always panicky about things and not taking time to analyse and see the big picture to make real money.

First, obviously we know how to host. Just for sites you know we own, we have Maxconsole, Team-xecuter etc. which are 1000 times more traffic than your site ever had. Second, of course[,] Axiogame will be back up, it is already back but we have some issues which I am trying to understand.

Axiogame has over 200 orders per day . . .

1 113. On or about August 23, 2017, after receiving an email from LOUARN
2 inquiring whether BOWSER knew anyone who could write a review about the Stargate
3 circumvention device on maxconsole.com, BOWSER provided the address of a potential
4 reseller that wanted a review sample. BOWSER also noted that they needed a “new
5 major usa/Canada reseller” because their prior reseller could “no longer touch Nintendo
6 products because of their flashcart settlement” with Nintendo.

7 114. On or about November 30, 2017, LOUARN sent an email to a developer
8 instructing him that he could use email to communicate with LOUARN regarding
9 legitimate products but should always use PGP encryption to communicate about hacking
10 projects.

11 115. On or about December 26, 2017, LOUARN and CHEN exchanged emails
12 regarding the financing of the initial production run for the Classic2Magic circumvention
13 device.

14 116. On or about December 28, 2017, BOWSER sent LOUARN an email
15 stating, “in regard to the Xbox One project[,] everything is in place, now we need you
16 onboard to discuss money, etc.”

17 117. On or about January 30, 2018, LOUARN sent CHEN an email requesting
18 money for the conspiracy’s developers, which read in part:

19 the team (for SG, N2 and soon the Wii chip) is asking me for funds to pay
20 for dev and parts. I told them we are really tense now, but that [I] will do
21 my best. are you able to take some preorders or something to pay them, as
22 he told me he really needs cash badly to pay for some parts and mostly to
keep the devs happy as they work hard on the wii chip.

23 118. On or about March 22, 2018, LOUARN sent CHEN an email attaching a
24 document that described the planned packaging of a circumvention device. The
25 attachment explained that the device was “basically a ‘clone’ of snes mini classic with
26 much more games.” The attachment further explained that the packaging designer should
27 “keep the style of the original snes mini classic, but different fonts, or enough difference,
28 so Nintendo doesn’t complain.”

1 119. On or about June 13, 2018, LOUARN forwarded CHEN an email
2 complaint from a customer who had ordered an SX Pro from a reseller but never received
3 the circumvention device, which read in part: "another crappy site by crappy reseller.
4 please speak with them to fix their form and reply to the guy."

5 120. On or about August 17, 2018, BOWSER sent an email explaining:
6 The C2M official launch is going well, lots of feedback, this is going to be
7 [a] very popular device, might even end up more popular th[a]n the Switch
8 stuff since its also 'mainstream' product more legit, . . .

9 121. On or about August 14, 2018, BOWSER communicated with a reseller of
10 Team Xecuter-branded products regarding advertising space that the reseller purchased
11 on maxconsole.com. Specifically, the reseller requested that BOWSER update the link in
12 the advertisement. The reseller explained that enforcement actions by Nintendo had
13 resulted in the takedown of some of the reseller's domain names.

14 122. On or about August 18, 2018, BOWSER sent an update regarding the
15 Classic2Magic device. Specifically, BOWSER noted "I [am] going to be busy setting up
16 the 'underground' stuff (rompacks, coverarts, emulators) on maxconsole forums, that will
17 also help on 'grey side' of the device for those wishing to play more than original snes
18 cartridges . . ."

19 123. On or about August 24, 2018, BOWSER sent an email to prospective
20 business partners that provided a status report regarding Team Xecuter's various projects.
21 BOWSER indicated that the conspiracy was responding to enforcement efforts focused
22 on removing ROMs from the internet:

23 They have been trying hard to crack down on everything, removing 'roms'
24 from various sites which devices like Classic2Magic need, but we have [a]
25 plan in the works to have secure links to these retro rompacks on [a]
protected server, so it will not be a problem.

26 BOWSER also explained that Team Xecuter was working to add a feature to the SX OS
27 that would allow users to play ROMs for older consoles on the Switch:

28 Next up on [the] roadmap of updates to SX OS is v1.7[;] this one will
include something called 'Retro SX', basically core emulators of other

1 older consoles, NES, SNES, Gameboy, DS, etc. so you will be able to play
2 backup roms of older Nintendo games, and later on some other older
3 consoles, this will also be exclusive to SX OS which again like the 'cheats'
above will keep the marketplace open for more sales of license keys . . .

4 In a subsequent email, sent on or about October 15, 2018, BOWSER reported that the
5 Retro SX project "blew up in our face" because the developer who had been paid to work
6 on the project had sent his work to a rival hacking group.

7 124. On or about September 13, 2018, BOWSER sent an email detailing the
8 conspiracy's development of a variety of circumvention devices including the SX OS, SX
9 GEAR, and the Classic2Magic. BOWSER explained that the conspiracy was developing
10 a project, titled "700 in 1," which would be the conspiracy's own version of the
11 Nintendo's SNES Mini but would have 700 games pre-installed. BOWSER also
12 explained that the conspiracy planned to develop a circumvention device for Microsoft's
13 XBOX One console:

14 The last big console that really does not have anything for it, is of course
15 Xbox One, it[']s been on [the] back burner for a while, but now with
16 Switch basically completed and sales moving along, it is time to bring this
back into focus and build up a solid, tight, team that can handle it . . .

17 125. On or about September 19, 2018, BOWSER sent an email to a known
18 modchip distributor indicating that "[w]e are soon (starting this week) going to be
19 offering special ads on the main TX site: --> <https://team-xecuter.com/> . . ." BOWSER
20 explained the "ads will be limited offering under 'recommend[ed] resellers" and that the
21 ads could not "showcase other non-TX products, and if possible must link directly to the
22 'TX/SX Family' listing of all those products only."

23 126. In or about October 2018, BOWSER sent emails soliciting paid
24 advertisements on a Team Xecuter website. On or about October 10, 2018, an individual
25 responded that he would not be advertising his website on the Team Xecuter website
26 because Nintendo had "been paying attention recently" to his website, thereby requiring
27 him to keep things "low key."
28

1 127. On or about October 16, 2018, BOWSER circulated an announcement for
 2 an update to the SX OS. The announcement advertised a new feature that would allow
 3 users to load ROMs and other content from external hard drives:

4 Yes. You read it right. You can now plug a USB mass storage device into
 5 your switch'[s] dock and load XCI or install NSP content from there
 6 directly. No longer are you limited by the size of your microSD card when
 7 playing the switch from the comfort of your couch, but you can now enjoy
 8 TERABYTES of content by using external harddisks and such!

9 128. On or about January 18, 2019, LOUARN sent CHEN an email attaching a
 10 spreadsheet containing the "first 1950 licenses" for the SX OS.

11 129. On or about October 16, 2019, BOWSER sent an update regarding attempts
 12 to evade Nintendo's enforcement actions as it pertained to circumvention devices.
 13 Specifically, in discussing where to place the conspiracy's servers, BOWSER noted that
 14 "dmca . . . only effects the usa and not other countries." He went on to explain that Team
 15 Xecuter intended to "stop using cloudflare which is usa-based, and to find another"
 16 similar service to obscure the location of the true servers, "mak[ing] it harder for
 17 [Nintendo] to get court order to find out the new server location and country." Team
 18 Xecuter also planned to remove reseller advertisements on the conspiracy's websites so
 19 the conspiracy is "not seen as 'promoting' the product directly, and leaving it up to the
 20 customer on his own to find a place that sells [the device.]" BOWSER even discussed
 21 placing a "fine-print" disclaimer "to make the customers understand they are not buying
 22 an authorized product and that it may or may not be legal in their country, etc."

23 All in violation of Title 18, United States Code, Section 371.

24 **COUNTS 7-10**

25 **(Trafficking in Circumvention Devices)**

26 130. The factual allegations set forth in Paragraphs 1 through 95, and 111
 27 through 129 of this Indictment are re-alleged and incorporated as if fully set forth herein.

28 131. On or about the dates identified below, at Seattle, within the Western

District of Washington, and elsewhere, the defendants, MAX LOUARN, aka "MAXiMiLiEN", aka "Julien Ambroise," YUANNING CHEN, aka "Yuan Ning Chen," aka "Velison Chen," aka "100+1," aka "Jingui Chen," and GARY BOWSER, aka "GaryOPA," did knowingly and willfully, and for purposes of commercial advantage and private financial gain, manufacture, import, offer to the public, provide, and traffic in a technology, product, service, device, component, or part thereof, that was primarily designed and produced for the purpose of circumventing a technological measure that effectively controlled access to a work protected under Title 17 of the United States Code, namely videogames, as set forth below:

| Count | Approximate Dates | Circumvention Device |
|-------|--------------------------------|----------------------|
| 7 | June 2013 to August 19, 2020 | Gateway |
| 8 | August 2017 to August 19, 2020 | Stargate |
| 9 | May 2018 to August 19, 2020 | SX OS and SX Pro |
| 10 | August 2018 to August 19, 2020 | Classic2Magic |

All in violation of Title 17, United States Code, Sections 1201(a)(2)(A), and 1204(a)(1), and Title 18, United States Code, Section 2.

COUNT 11
(Conspiracy to Commit Money Laundering)

132. The factual allegations set forth in Paragraphs 1 through 106 and 111 through 129 of this Indictment are re-alleged and incorporated as if fully set forth herein.

133. Beginning at a time unknown, but no later than June 2013, and continuing through August 19, 2020, at Seattle, within the Western District of Washington, and elsewhere, MAX LOUARN, aka "MAXiMiLiEN," aka "Julien Ambroise," YUANNING CHEN, aka "Yuan Ning Chen," aka "Velison Chen," aka "100+1," aka "Jingui Chen," and GARY BOWSER, aka "GaryOPA," and others known and unknown to the Grand Jury, did knowingly combine, conspire, and agree with each other and with other persons

1 known and unknown to the Grand Jury to commit offenses against the United States in
2 violation of Title 18, United States Code, Section 1956, to wit:

3 a. to knowingly engage and attempt to engage, in monetary
4 transactions by, through or to a financial institution, affecting interstate and foreign
5 commerce, in criminally derived property of a value greater than \$10,000, such property
6 having been derived from a specified unlawful activity, that is, wire fraud, in violation of
7 Title 18, United States Code, Section 1343, conspiracy to commit wire fraud, in violation
8 of Title 18, United States Code, Section 1349, and copyright infringement, in violation of
9 Title 18, United States Code, Section 2319(b)(1), in violation of Title 18, United States
10 Code, Section 1957.

11 b. to knowingly conduct and attempt to conduct financial transactions
12 affecting interstate commerce and foreign commerce, which transactions involved the
13 proceeds of specified unlawful activity, that is, wire fraud, in violation of Title 18,
14 United States Code, Section 1343, conspiracy to commit wire fraud, in violation of Title
15 18, United States Code, Section 1349, and copyright infringement, in violation of Title
16 18, United States Code, Section 2319(b)(1), knowing that the transactions were designed
17 in whole or in part to conceal and disguise the nature, location, source, ownership, and
18 control of the proceeds of specified unlawful activity, and while conducting and
19 attempting to conduct such financial transactions, knew that the property involved in the
20 financial transactions represented the proceeds of some form of unlawful activity, in
21 violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

22 All in violation of Title 18, United States Code, Section 1956(h).
23

24 **FORFEITURE ALLEGATIONS**

25 **Conspiracy to Commit Wire Fraud and Wire Fraud**

26 134. The factual allegations contained in Paragraphs 1 through 106 of this
27 Indictment are realleged and incorporated by reference for the purpose of alleging
28 forfeiture.

135. Upon conviction of any of the offenses charged in Counts 1 – 5 of this Indictment, the defendant, MAX LOUARN, aka “MAXiMiLiEN,” aka “Julien Ambroise,” YUANNING CHEN, aka “Yuan Ning Chen,” aka “Velison Chen,” aka “100+1,” aka “Jingui Chen,” and GARY BOWSER, aka “GaryOPA,” shall each forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C), by way of Title 28, United States Code, Section 2461(c), any property that constitutes or is traceable to proceeds he obtained from the offense. This property includes, but is not limited to, a sum of money reflecting the proceeds each Defendant obtained from the offense.

Money Laundering Conspiracy

136. The factual allegations contained in Paragraphs 132 through 133 of this Indictment are realleged and incorporated by reference for the purpose of alleging forfeiture.

137. Upon conviction of the offense charged in Count 11 of this Indictment, the defendants, MAX LOUARN, aka “MAXiMiLiEN,” aka “Julien Ambroise,” YUANNING CHEN, aka “Yuan Ning Chen,” aka “Velison Chen,” aka “100+1,” aka “Jingui Chen,” and GARY BOWSER, aka “GaryOPA,” shall each forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), any property that constitutes or is traceable to proceeds he obtained from the offense, as well as any property involved in the offense. This property includes, but is not limited to, a sum of money reflecting the proceeds each Defendant obtained from the offense.

(Substitute Assets)

138. If any of the property described above, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or

1 e. has been commingled with other property which cannot be divided
2 without difficulty,
3 the United States of America shall be entitled to forfeiture of substitute property pursuant
4 to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States
5 Code, Section 2461(c).

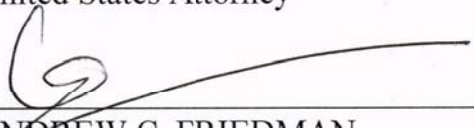
6 A TRUE BILL:

7 DATED: *August 19, 2020*

8
9 *(Signature of Foreperson redacted pursuant to*
10 *policy of the Judicial Conference)*


11 FOREPERSON

12 
13 BRIAN T. MORAN
14 United States Attorney

15 
16 ANDREW C. FRIEDMAN
17 Assistant United States Attorney

18 
19 FRANCIS FRANZE-NAKAMURA
20 Assistant United States Attorney

21 
22 BRIAN WERNER
23 Assistant United States Attorney
24
25
26
27
28


BRIAN C. RABBITT
Acting Assistant Attorney General


FRANK LIN
Senior Counsel